Opening Statement for U.S. House of Representatives, Committee On Science

April 28, 2004

James J. Jasinski
Vice President, Cogent Systems, Inc.

STATEMENT

Thank you for the opportunity to appear before this Committee on Science to review Cogent's experience working with the NIST, to articulate the success derived from that association, and to identify how that success can continue and in fact grow.

Cogent is an American company founded 14 years ago by US citizens. Our corporate headquarters is in South Pasadena, California with affiliated offices in 5 countries. From our corporate headquarters we have deployed Automated Fingerprint Identification Systems (AFIS) at the national, state and local levels. This includes over 45 foreign countries, such as the United Kingdom, Italy, Bulgaria, Russia, Taiwan, Hong Kong, Singapore, Honduras, Algeria, and dozens of others providing us a presence on five continents. Traditionally, 4 major AFIS companies have serviced this market. Of these 4 companies, one other is US based and the remainder are foreign corporations.

The focus of this statement is on two primary topics:

1) NIST's role in establishing fingerprint interoperability within the United States and around the world;
2) NIST contributions to the universally acknowledged successful deployment of the US VISIT Program.

1) Interoperability Standards

The history of AFIS technology in many ways mirrors that of technology in general i.e. the evolution from proprietary standards to open standards. Just like in the 1970s, the purchase of one information mainframe system meant the inability to interoperate with that of a competitor, the AFIS users found themselves in a similar situation. This meant that someone arrested in one State could not have his fingerprints automatically searched against fingerprint records of another State. This clearly was unacceptable. Therefore, when the Federal Bureau of Investigation (FBI) undertook its Integrated Automated Fingerprint Identification System (IAFIS) project, open standards had to be developed to ensure that upon the completion of IAFIS the States and the FBI would be able to routinely exchange fingerprint information.

NIST provided the nexus between the system developers and the end users of the systems that allowed the development and acceptance of open standards for exchanging fingerprint information. Today, in the AFIS community, all major government sponsored AFIS acquisitions require any proposed AFIS solution must be “NIST Compliant.” “NIST Compliance” is shorthand for approximately 15 standards dealing with fingerprints---from the header, to the image quality, to compression, to today the complete palms. These standards have been openly reviewed, developed, and deployed by all parties working in this area and have been universally accepted. As a result, around the world today, AFIS systems are routinely interoperable at the system level. While, these standards allow the systems to work together, at the same time they protect the uniqueness of each system and the investment each company has put into its technology.

As illustrative of the success of those NIST standards, while I was in the FBI, I chaired Interpol’s AFIS Expert Working Group. At that time Interpol was acquiring an AFIS system for itself and for interfacing with over 100 members. The solicitation for that procurement required “NIST Compliance” for any vendor proposed system. The value of such a system is proven everyday when countries around the world exchange their fingerprint data with one another---all because of NIST leadership.

2) US VISIT

For many years the US has been aware of the problem of tracking visitors to the United States. As part of the initial efforts to try and establish a process for such a tracking system, Homeland Security announced on April 29, 2003 a plan to begin establishing a biometric system to perform this task by the end of 2003. In establishing this system, a number of issues sprung up; how many fingers were necessary ---from 2,4,6,8,10, should they be rolled or flat captures, can a database of mixed flat and rolled fingers be accurately searched, operational accuracy, as well as a host of other related issues.

At this time, a series of inaccurate, wrong, deceptive and self- serving representations were made by a number of alleged biometric experts. Each sounded authoritative and knowledgeable, but each had more theory than reality in their pronouncements. This complicated any decision to proceed with this too often delayed national defensive system for if the critics were right, millions of dollars would be wasted. Fortunately, NIST helped resolve the outstanding issues and validate operational feasibility so US VISIT could be deployed. Before discussing NIST’s role in resolving these issues, please let me take a few moments to provide some background information on AFIS systems.

In assessing the performance of a system you look at four major factors:

1) Accuracy;
2) Database size/composition;
3) Number of fingers searched;
4) Throughput—how many comparisons can be done in a set time.

In AFIS technology accuracy is a term of art. Accuracy has two sides---finding someone in a database (called “reliability”, “Type1 Rate”, “True Acceptance Rate “ (TAR)) and falsely finding someone (called “selectivity”, Type 2 Rate”, “False Acceptance Rate” (FAR). These accuracy rates are a set of measures used to understand the performance of the system with respect to the system’s ability to correctly process the presences or absence of an individual’s fingerprints in a database. Therefore, the terminology is as follows:

- Accuracy is the measure of ability of the system to correctly match the fingerprints of an individual to that person’s fingerprints in the database.
- Type 1 Errors, also known as False Reject or False Non-Match is the measure of the system’s inability to correctly match a set of fingerprints to a mating set of fingerprints that are in the database.
- Type 2 Errors, also known as False Accept or False Match is the measure of the system’s inability to correctly differentiate between a set of fingerprints and another set of fingerprints within a database.

AFIS systems are impacted by the amount of data, the quality of the images, and whether what is stored is a rolled or flat fingerprint image. The size of the database determines how much time is necessary to determine if there is or isn’t a match. In making that comparison, the quality of the images either being searched or stored significantly affect search results. As NIST has stated, 35 bad images are not as valuable as 1 good one. Then, for most AFIS systems, whether the image is rolled or flat or whether they are intermixed will impact search results.

Additionally, how many fingers that are searched will impact system accuracy. As a general rule, more quality images are better than fewer quality images, but results are not linear. That means one cannot project that a search of a finger with certain results proportionately improves with each additional finger searched. Rather accuracy is a function of many factors such as the design of the search process, the quality of the images, the time for the search etc.

Finally, AFIS systems performance are impacted by throughput--- how many transactions do you need to process within a set amount of time. Frequently, to achieve greater throughput accuracy is sacrificed.

In assessing the performance of an AFIS system the above factors must be balanced with the application environment in determining effectiveness.

When US VISIT was announced, a number of companies, foreign and domestic, immediately attacked the biometric approach. Their representations were presumptive and unfounded, but because of their position in the market, given credibility. As the US VISIT system was being developed, with the proposed approach to expanding the proven technology used by DHS for its IDENT program, a number of inaccurate reports and statements became common in newspapers, trade periodicals, and commentaries. For example, a leading system integration organization issued a White Paper to DHS that made the following comments regarding the plan to use IDENT technology for US VISIT:

> “However, the current IDENT system has not been proven to meet the IDENT system Accuracy & Type 1 Error Rate requirements and further is believed to fall substantially below expected Accuracy. The engineering estimate values used in this evaluation were 75% accuracy, 25% Type 1 Error Rate and 0.6% Type 2 Error Rate.”

Such assessments raised unfounded concerns about the viability of the biometric deployment for US VISIT, for if accurate would essentially mean an unacceptable low reliability rate of 75% with every fourth traveler being sent to a secondary examination.

The above White Paper then went to state:

> **“**As the current IDENT system is not meeting Accuracy and Type 1 Error Rate specification,….. The spreadsheet contains an engineering estimate of the real values. The engineering estimate is based on an extrapolation of the independent Criminality Study as well as a small ad-hoc system test…… This data was not truly randomly sampled and had a quantity of low quality data removed from the set. Those factors skewed the results indicating higher Accuracy than is believed to be truly available in the current environment. A further indication that the values were skewed was that these values taken together as an “operational point” represent a significantly higher capability than is currently published as state-of-the-art for commercially available AFIS systems. These “best measured” values were not developed from a realistic test and are not believable…

This report was based upon based the Systems Integrator’s knowledge of their AFIS system’s capability coupled with a flawed mathematical calculation in the referenced criminality report.

That criminality report was published in October 2000 entitled IDENT/IAFIS IQS. Cogent had no participation in that report and as a result the basis for the number comes from **IAFIS** results of a 2 fingers search using the **IAFIS** system --- ***not the Cogent IDENT system***. Of particular note, in calculating the number of Cogent errors, the report did not convert the measured Type 2 error rate of .16% correctly as they did not convert the type 2 percentage to a decimal number.

In addition, other alleged experts were heavily spreading misinformation on the proposed system’s overall performance and falsely charging an inability to grow with the workload.

Given this context, NIST was tasked to validate the system—from accuracy to throughput. NIST timely performed its mission. However, in performing this testing NIST stretched its equipment capacity as shown by running CPUs at 100% utilization, storage contentions, database management software licenses, and using old chemical labs instead of computer facilities to perform the testing. Their successful testing of the system and repudiation of the many false statements allowed the scheduled deployment to proceed as announced. This means a safer America for with the system in place, since January 5, 2004, hundreds of individuals have been identified for further investigation prior to their being allowed to enter this country. Some are subsequently banned from entering, some are arrested and some are allowed entry, however each determination is made with the greater certainty than was ever before deemed possible. In fact one Immigration officer described the system as “a wonderful Christmas gift”.

Even today, after the successful implementation of US VISIT, the same critics who predicted system failure and performance problems continue to push their less than honest agenda. To be sure, all systems are a balancing between operational requirements, business procedures, and acceptable performance characteristics. No one would argue that more data is better than less data, however the context for that question is what is the impact to your business processes in acquiring that additional data, what is its cost, and what are its advantages. In making those judgment calls, NIST must continue to perform the roll of the honest broker so that Agencies understand what are the true trade offs for the final decision in implementing biometric technology.

For example, with US VISIT, the decision to capture more fingers in future applications must trade off the additional equipment and labor costs in capturing those fingers with the improvements to the TAR (reliability) and the FAR (selectivity) with less manpower in the backend of the system. To date, NIST has shown that the TAR for a 2 print system remains constant as the system grows, at least for the limits of its available database size of about 6 million subjects, while the FAR rises in a predictable linear fashion. That same testing has shown that good images are more important for the system’s TAR/FAR results than multiple bad images taken from the same person. Simultaneously, the testing has shown that more fingers does increase the probability of obtaining more usable data and that FAR levels can be essentially maintained as the database grows. Additionally capturing more fingers allows for sequence checking and is of greater value for latent searches. All of this is subject to current NIST database sizing limitations and highlights the continuing important role for NIST in US VISIT.

This is but an example of the importance of their role in validating technology claims and clearly indicates the importance of increasing and enhancing that role. As technology grows within society the resources required to validate them correspondingly grow. Illustrative is the Fingerprint Vendor Technology Evaluation (FpVTE) 2003. That evaluation addressed system performance of fingerprint matching algorithms. It required significant equipment, vast amounts of data, and knowledgeable personnel to perform the evaluation. Due to resource limitations the scope of the test was restricted to areas that NIST could independently validate with its available resources. That means that the test could measure only targeted areas not total system performance. And even in performing the targeting testing, because of resource limitations ranging from equipment to data, the testing could not empirically validate all of its target performance objectives but rather had to defer to extrapolations of data.

Cogent believes that if NIST was appropriately funded, NIST can perform fuller and more robust empirical testing of systems, technologies, and theories. With that additional funding, instead of merely testing a target objective, it can perform empirical system testing of products that could not only demonstrate American technology, but assist in keeping its leadership by either exposing or disproving unreliable systems.